УДК 336.71

ПОТЕРИ БАНКОВ ОТ КИБЕРПРЕСТУПНОСТИ

***Яшутина Д.С.*[1]**

студент,

Финансовый университет при Правительстве Российской Федерации,

Москва, Россия

Аннотация

В статье рассматриваются проблемы кибербезопасности в банковском секторе. В ходе работы раскрывается специфика киберпреступности, проводится анализ масштабов ее проникновения в деятельность кредитных организаций на территории Российской Федерации. На основании проведенного исследования автор отмечает значительную угрозу кибератак для банковского сектора и приводит ряд мер, позволяющих минимизировать негативные последствия данного рода преступления.

Ключевые слова: банки, банковский сектор, высокие технологии, киберпреступность, информационная безопасность.

BANK LOSSES FROM CYBERCRIME

Yashutina D.S.

student,

Financial University under the Government of the Russian Federation,

Moscow, Russia

[1] *Научный руководитель: **Александрова Л.С.**,к.э.н., доцент, Финансовый университет при Правительстве Российской Федерации, Москва, Россия*

Abstract

The article considers the problem of cybersecurity in the banking sector. During the work the specifics of cybercrime were revealed and the scale of its penetration into the activities of credit institutions in the Russian Federation was analyzed. On the basis of their studies, the author notes a significant threat of cyberattacks to the banking sector and provides a number of measures to minimize the negative consequences of this type of crime.

Keywords: banks, banking sector, high technologies, cybercrime, information security.

В настоящее время информационные технологии имеют достаточно обширную область применения. Банковская сфера также не является исключением. Всеобщая информатизация и компьютеризация банковской деятельности позволяет повысить оперативность проведения различного рода банковских операций и снизить затраты на их осуществление, иными словами, создать благоприятную среду для эффективной и результативной работы кредитных организаций. Однако активная цифровизация банковских операций повлекла за собой и развитие преступности в IT-сфере. Причина состоит в повсеместном распространении электронных платежей, в результате чего денежные средства не только банков, но и их клиентов стали объектом информационных атак. Несмотря на то, что банки стараются обеспечить надежную и бесперебойную защиту электронно-вычислительных систем, хакеры изобретают новые схемы, позволяющие им обойти имеющуюся у банков систему информационной безопасности.

Именно поэтому на сегодняшний день остро стоит вопрос о кибербезопасности кредитно-банковской сферы. С внедрением высоких технологий возник и получил широкое распространение совершенно новый вид преступности под названием киберпреступность. Его специфика состоит

в том, что достаточно сложно определить наличие и состав самого преступления, а особенно – виновных в его совершении. Трудность выявления подобного преступного деяния обусловлена характерными для него особенностями, которые в определенной степени отражают его сущность [1]:

- латентность – максимально возможная скрытость преступления, обеспечивающаяся механизмом шифрования, анонимности и кодирования;
- трансграничность, обусловленная дистанционностью положений виновных и пострадавших лиц;
- автоматизированный режим – реализация всех необходимых процедур обработки информации при минимальном участии человека.

При совершении киберпреступлений хакеры в качестве основной цели преследуют хищение денежных средств как самих кредитных организаций, так и их клиентов с использованием различных уникальных схем, таких как троянские программы, через которые мошенники могут вредоносно воздействовать на банковскую информационную систему; прием социальной инженерии, позволяющий киберпреступникам «играть» на человеческих слабостях; фишинг, в основе которого заложено создание точной копии банковского сайта и тем самым получение доступа к конфиденциальной информации, и заключительный метод – скимминг, подразумевающий кражу данных карты через банкоматы с использованием специальных считывающих устройств. Все перечисленные типы кибермошенничества представляют большую угрозу для банковского сектора, ведь ущерб, который они могут нанести кредитным организациям, достаточно велик.

По данным отчета международной компании по предотвращению и расследованию киберпреступлений, Group-IB, потери российских банков с середины 2018 года по середину 2019 года составили 510 млн рублей, что на 85% меньше аналогичного периода 2017-2018 годов, в который данный

показатель достигал 3,2 млрд рублей [2]. За время проведения исследования были выявлены случаи хакерских атак, охватившие следующие сегменты российского рынка: хищение средств у физических и юридических лиц, однако у первых – с Android троянами, у вторых – с троянами для ПК, целевые атаки на банки, фишинг и обналичивание похищаемых средств – денежный объем реализации подобного рода киберпреступлений представлен ниже (таблица 1).

Таблица 1 – Оценка Group-IB рынка высокотехнологичных преступлений в финансовой отрасли России

Сегмент рынка в России	Сумма хищений, тыс. рублей
Хищение у юридических лиц с троянами для ПК	62 250
Хищение у физических лиц с Android троянами	109 560
Целевые атаки на банки	93 000
Фишинг	86 652
Обналичивание похищаемых средств	158 158
Итого	509 620

По сравнению с предыдущим годом ущерб от целенаправленных атак на банки РФ сократился практически в 14 раз, что Group-IB связывает с переключением фокуса киберпреступников на кредитные организации иностранных государств.

В 2019 году специалистами Group-IB была зафиксирована атака со стороны новой группировки «RedCurl», которая в качестве основного метода совершения преступления использовала фишинг: злоумышленники использовали уникальную самописную троянскую программу, при помощи которой коммуникация с управляющим сервером осуществлялась через легитимные сервисы, что и затрудняло обнаружение вредоносной активности. Таким образом, потери от фишинговых атак за исследуемый период 2018-2019 годов составили около 87 млн рублей.

Также, несмотря на то, что из года в год количество применяемых троянов снижается за счет внедрения банковским сектором новых средств защиты и тем самым сокращения экономических выгод для атакующих,

такие программы полностью не исчезают и продолжают представлять угрозу для денежных средств физических и юридических лиц. Трояны для Android исчезают медленнее, чем для ПК, так как киберпреступники продолжают разрабатывать новые Android программы, которые за последние несколько лет эволюционировали от перехвата SMS к автоматическому переводу средств через банковские мобильные приложения. Именно поэтому хищения, осуществляемые таким методом, все еще занимают достаточно большую долю в потерях банковского сектора: за 2018-2019 годы они приблизительно равнялись 172 млн рублей в общей сумме для юридических и физических лиц.

В России также имеется свой центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, занимающийся анализом операций, совершаемых без согласия клиентов кредитных организаций, с целью их выявления и предотвращения. Данные задачи лежат в основе деятельности ФинЦЕРТ, специального структурного подразделения Центрального банка РФ.

Согласно официальным сведениям ФинЦЕРТ с 2015 года по 2017 год наблюдался тренд в сторону уменьшения общего объема несанкционированных операций: в 2017 году данный показатель сократился практически на 11% по сравнению с аналогичным периодом прошлого года (в 2016 году объем несанкционированных операций составил 1080 млн рублей и это было на 5% ниже показателя 2015 года) (рис.1) [3, 4, 5]. Как отмечает ФинЦЕРТ, данная тенденция связана с переориентацией мошенников с дистанционных платежных систем на информационные инфраструктуры операторов по переводу денежных средств и операторов услуг платежной инфраструктуры. Начиная же с 2018 года, заметна тенденция, связанная с увеличением объема несанкционированных операций: за 2018 год киберпреступники украли у клиентов банков России 1 384,7 млн рублей - на 44% больше, чем в 2017 году. На следующий год объем

несанкционированных операций составил 5 723,5 млн рублей, что значительно большего показателя 2018 года (в 2019 году объем несанкционированных операций увеличился в 4 раза по сравнению с 2018 годом) [6, 7]. При этом количество подобного рода операций возрастало на протяжении пяти лет.

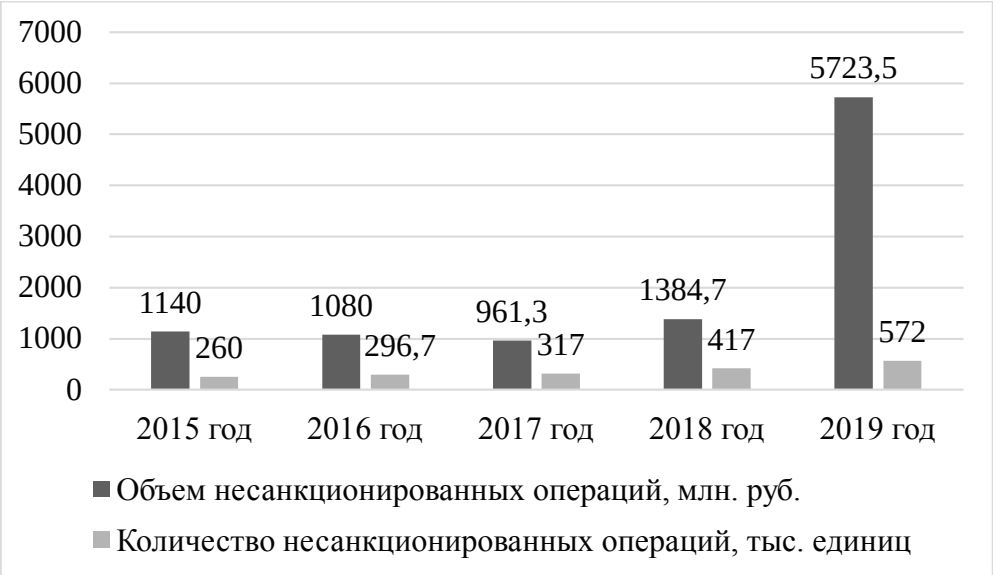

Рис.1 – Количество и объем несанкционированных операций

Относительно 2019 года информационные атаки со стороны киберпреступников осуществлялись на основании проведения следующих операций:

- операции через банкоматы, терминалы и импринтеры;
- оплата товаров и услуг в Интернете (CNP-транзакции);
- операции в системе дистанционного банковского обслуживания (ДБО).

Активное развитие платежных сервисов с применением современных информационных технологий способствует расширению сферы безналичных расчетов, все больше приобретающих доминирующее положение в денежном обороте. Таким образом, повышается доступность платежных услуг, в результате чего хакеры перенаправляют свои действия от банкоматов торговли в сторону CNP-транзакций, каналов ДБО. Официальные сведения

исследований ФинЦЕРТ подтверждают миграцию операций без согласия клиентов в CNP-среду (рис.2).

Рис.2 – Типы операций, совершенных без согласия клиентов, и их доля в общем количестве всех совершенных несанкционированных операций

Необходимо отметить, что основная часть операций без согласия клиентов, а именно физических лиц, реализовывалась посредством методов социальной инженерии. Банки возместили своим пользователям 935 млн рублей, что составляло лишь 15% похищенных средств, так как клиенты, подвергаясь обману со стороны киберпреступников, нарушали условия договора с кредитными организациями, закрепляющими за ними сохранение конфиденциальности платежной информации. В связи с рядом подобных случаев Банк России намерен рассмотреть возможности по повышению финансовой грамотности граждан в части обеспечения безопасности применяемых информационных и платежных технологий. Однако в наличии имеются и факты совершения несанкционированных процедур с использованием иных методов кибератак, в результате совершения которых у клиентов могут сформироваться сомнения по поводу безопасности дистанционных банковских сервисов. Именно поэтому кредитные организации обязаны обеспечить эффективную систему информационной

безопасности в банковском секторе и принять соответствующие меры, способствующие минимизации риска осуществления киберпреступлений [8]. Риск несоблюдения правил конфиденциальности данных может возрасти с развитием больших данных, большим объемом аутсорсинга из-за связей банков с FinTech-компаниями и связанной с этим борьбой за право собственности на отношения с клиентами.[9, с. 181]

На сегодняшний день Центральный банк РФ в качестве основных направлений своей деятельности в области информационной безопасности ставит следующие задачи [10]:

1. Обеспечение киберустойчивости за счет таких составляющих, как:

- готовность кредитно-финансовой сферы гарантировать операционную надежность и финансовую стабильность предоставления финансовых и банковских услуг, в особенности – при условиях реализации различного рода информационных атак;
- контроль за показателями риска реализации информационных угроз со стороны злоумышленников, а также уровня несанкционированных операций без согласия клиентов;
- мониторинг, оперативное реагирование и предотвращение кибератак на кредитные организации.

2. Защита права пользователей финансовых услуг через систему мониторинга показателей нанесенного кредитным организациям финансового ущерба.

3. Содействие развитию ИКТ в области контроля за показателями риска реализации информационных угроз и обеспечение надлежащего уровня информационной безопасности.

Благодаря принимаемым на период 2019-2021 годов Банком России мерам защитного характера повышаются шансы российских банков предотвратить финансовые потери, нарушения операционной надежности и

непрерывности предоставления финансовых услуг, вероятность наступления системного кризиса в случае возникновения инцидентов информационной безопасности в результате кибератак. Однако на законодательном уровне также разработан механизм по предотвращению различного рода мошенничества в различных платежных системах, связанного с использованием электронных средств платежа: в статье 159.3 Уголовного Кодекса Российской Федерации предусмотрен штраф, ограничение или лишение свободы – вид наказания будет зависеть от размера, в котором было совершено деяние, и отдельных его составляющих [11].

Изучив особенности киберпреступности, а также проанализировав ущерб банковского сектора от хищений платежных средств подобным образом, можно сделать вывод, что потери банков в результате совершенных хакерских атак весьма велики, что в определенной степени дестабилизирует деятельность кредитных организаций. Из-за новизны таких преступлений и их высокого уровня доходности, невозможно осуществить их полную ликвидации, однако необходимо уметь найти эффективные методы, позволяющие минимизировать последствия киберпреступности или вовсе исключить факт их реализации, тем самым появляется возможность снизить уязвимость банковского сектора и его инфраструктуры, чем и занимается Банк России.

Библиографический список:

1. Литвинов, Д.А. Киберпреступность в банковской сфере России: характер, масштабы, последствия / Д.А. Литвинов // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. — 2017. — № 1. — С. 35-42 [Электронный ресурс]. — Режим доступа — URL: https://www.elibrary.ru/download/elibrary_30010421_10141122.pdf (Дата обращения: 15.11.2020)

2. Топ-10 тенденций из нового отчета High-Tech-Tech Crime Trends 2019/2020 Group-IB [Электронный ресурс]. — Режим доступа — URL: https://habr.com/ru/company/group-ib/blog/477958/ (Дата обращения: 15.11.2020)

3. Обзор о несанкционированных переводах денежных средств за 2015 год // Банк России [Электронный ресурс]. — Режим доступа — URL: https://cbr.ru/Content/Document/File/106014/survey_2015.pdf (Дата обращения: 15.11.2020)

4. Обзор несанкционированных переводов денежных средств за 2016 год // Банк России [Электронный ресурс]. — Режим доступа — URL: https://cbr.ru/Content/Document/File/84814/survey_transfers_16.pdf (Дата обращения: 15.11.2020)

5. Обзор несанкционированных переводов денежных средств за 2017 год // Банк России [Электронный ресурс]. — Режим доступа — URL: https://cbr.ru/Content/Document/File/84813/survey_transfers_17.pdf (Дата обращения: 15.11.2020)

6. Обзор несанкционированных переводов денежных средств за 2018 год // Банк России [Электронный ресурс]. — Режим доступа — URL: https://cbr.ru/Content/Document/File/62930/gubzi_18.pdf (Дата обращения: 15.11.2020)

7. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год // Банк России [Электронный ресурс]. — Режим доступа — URL: https://cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (Дата обращения: 15.11.2020)

8. Гамза В. А. Безопасность банковской деятельности: учебник для вузов / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 5-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 455 с. [Электронный ресурс]. —

Режим доступа — URL: https://urait.ru/bcode/467446/p.2 (Дата обращения: 15.11.2020)

9. Банки и финтех-компании: взаимодействие и конкуренция: монография. -/Под ред. Л.С.Александровой – Москва: РУСАЙНС, 2020.

10. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов // Банк России [Электронный ресурс]. — Режим доступа — URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf (Дата обращения: 15.11.2020)

11. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.10.2020) // Собрание законодательства РФ. — 17.06.1996. — № 25. — ст. 2954 [Электронный ресурс]. — Режим доступа — URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (Дата обращения: 15.11.2020)

Оригинальность 87%